SEARCHING METHOD FOR A SECURITY POLICY DATABASE

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to Internet Protocol Security (IPSec), and particularly, to a searching method for a Security Policy Database (SPD).

2. Description of the Prior Art

The Virtual Private Network (VPN) applies the technology of the Internet Protocol (IP) to build the encryption tunneling on the Internet so as to establish the enterprise network on the Internet. The network based on the Internet protocol has good expandability, and applies the standard IPSec to be the protection technology. The IP security (IPSec, RFC 2401) combines the security standards of encryption, authentication, key management, digital certification, and so on so as to provide the high protection ability.

When the IPSec is applied for executing the data transmission, the processing can be inbound processing or outbound processing according to the direction of the data transmission. The inbound processing means that via the peer gateway, the data is transmitted from the peer network to the local gateway, and finally, to the local network. The packet received in the inbound processing is called as the inbound packet. There are two kinds of inbound packets. One is the inbound IPSec packet processed by the IPSec, and the other is the general inbound IP packet. The outbound processing means that via the local gateway, the data is transmitted from the local network to the peer gateway, and finally, to the peer network. The packet received by the outbound processing is called as the outbound packet, which is an outbound IP packet.

The IPSec has two different modes, the transport mode and the tunnel

mode. The transport mode is a host-to-host encapsulation mechanism, and the tunnel mode is a gateway-to-gateway or gateway-to-host encapsulation. In order words, a host supporting the IPSec has to support the transport mode and the tunnel mode, while the gateway only has to support the tunnel mode. However, the gateway can also support the transport mode so as to provide another selection to make the gateway directly communicate with the host.

The IPSec will determine which packets have to be processed according to the designated selectors, such as the network address, the protocol, and the port number in the SPD. The processing methods comprise applying the IPSec, by-passing the IPSec and discarding. The default processing method is directly discarding the packet. Also, in order to apply the IPSec, the user has to designate the mode of the IPSec, the protocol of the IPSec, the authentication algorithm, the encryption/decryption algorithm, and the key in the Security Association Database (SAD).

The SPD is an ordered list composed of different security policies. Each of the policies is selected according to different selectors. The selectors include the source address, the destination address, the protocol, the source port and the destination port. The range value of each of the selectors can be single, range or wildcard.

Because the selectors may be the same, the overlapping of the policies easily occurs. Namely, in the SPD, the selectors of more than two policies may equally match the searching requirement of one packet. Therefore, IPSec requires the searching of the SPD to be ordered. The searching has to start from the beginning policy and go on sequentially until the first policy matching with the requirement is found so as to obtain a consistent searching result.

Fig.1 is a perspective diagram of a prior art SPD. If the linear search is

directly applied to be the searching method for SPD, the time complexity is O(n), and n is the number of the policies. For the system having a greater number of policies, applying the linear search on the SPD will become the processing bottleneck of the IPSec. Nowadays, the number of the policies in the business product specification is below 100 for the families or small scale enterprises, about 1000 for the middle/large scale enterprises, and about 10000 for the very large scale enterprises.

In the prior art, in order to resolve the problem of searching the SPD, three methods are provided. The first one is the brute force parallel searching method. The second one is the flow-based searching method (disclosed in the US patent number 6,347,376, and the US patent publication number 2003/0023846 and 2003/0069973). Please refer to Fig.2. The third one is the Patricia-based searching method (disclosed in the US patent number 6,347,376 and the US patent publication number 2003/0061507). Please refer to Fig.3.

The brute force parallel searching method directly utilizes the capability of the hardware parallel processing. It divides the number of the policies of the system specification by the maximum number of the policies capable of being processed by a single SPD module so as to determine the number of the SPD modules to be duplicated. The policy manager will collectively manage the searching requirements of the inbound packet or the outbound packet, and then broadcast the requirement to the inbound SPD modules, or the outbound SPD modules for simultaneously searching, and then get the searching result back. If policies matching with the requirement are found out from more than two SPDs, the policy manager will choose the policy with highest priority and report it.

The drawback of this method is the high cost because multiple SPD modules have to be duplicated, and at most, only two searching requirements of

the SPDs can be served at the same time. One is the search for the inbound packets, and the other is the search for the outbound packets.

The flow-based searching method will perform some specific processes on each of the packet flow. Take the transport control protocol (TCP) packet for example, the packets having the same source address, destination address, protocol, source port and destination port belong to a packet flow. For the first packet of each of the packet flows, the linear search has to be performed on the SPD so as to obtain the corresponding policy. However, this method will store the search result for being used by the remaining packets in the same packet flow. If the search result is stored in a hash table of which the space usage rate is less than one half, theoretically, the time complexity is O(1).

However, the drawback of this method is that a great amount of memory space is required to maintain the hash table. The space complexity is O(f), and f is the number of packet flows. Furthermore, in this method, the linear search still has to be performed on the SPD for the first packet. Therefore, this may cause a period of delaying before the network program in the application layer builds the network connection.

The Patricia-based searching method applies the Patricia tree to search the data. The Patricia tree is a binary searching tree algorithm. The worst case of the Patricia tree having the non-contiguous masks is $O(w^2)$, and w is the length of the key of the Patricia tree. In the method disclosed in the US patent publication number 2003/0061507, w is 112. The drawback of the Patricia-based searching method is that the policies in the SPD cannot be overlapped. Otherwise another effective algorithm is required to transform the original SPD into a non-ordered SPD so that the search result can match the required order by the IPSec. However, in the prior art, the method for

transforming the security policy database into the non-ordered security policy database is not provided.

Fig.4 is a flowchart for processing a prior art outbound IPSec. As for the outbound IP packet (S10), the search is performed on the security policy database (S12). If the search result is "discard," then the packet is directly discarded (S11). If the search result is "by-pass," then go to the process for the Internet protocol (S13). If the search result is "apply," then search the security association database (S15). If not found, then discard the packet, and build the security association (S14). If found, encapsulate the outer header (S16), and then perform the encryption and authentication (S17). Thereafter, go to the process for the Internet protocol (S13).

Fig.5 is a flowchart for processing a prior art inbound IPSec. As for the inbound IPSec packet (S20), the search is performed on the security association database (S23). If not found (S22), then discard the packet. If found, perform the decryption and the authentication (S24), and then decapsulate the outer header (S25). Thereafter, the search is performed on the security policy database (S26). As for the inbound IP packet (S21), then directly search the security policy database (S26). If a wrong policy is found, then directly discard the packet (S22). If the correct policy is searched, then perform the process for the Internet protocol (S27).

SUMMARY OF THE INVENTION

The purpose of the present invention is to provide a searching method for a security policy database (SPD). According to one aspect of the present invention, the characteristic of peer gateway of the IPSec is applied to divide the original SPD into multiple smaller peer-based SPDs., and to build a peer

table corresponding to the peer-based SPDs so as to save the time for policy searching.

According to another aspect of the present invention, when searching for the policy, the selector of the policy, such as the source address or the destination address, is used for searching the peer table. In the peer table, the policy matching to the selector is corresponding to a peer identification, and the peer identification is corresponding to the peer-based SPD.

According to another aspect of the present invention, the present invention can be applied in the inbound packet, which is the inbound IPSec packet processed by the IPSec or the general inbound IP packet. The present invention also can be applied in the outbound packet, which is the outbound IP packet.

According to another aspect of the present invention, the present invention can be applied for IPSec in tunnel mode, and also can support IPSec in transport mode.

According to another aspect of the present invention, the present invention can be used by combining other searching methods, e.g. the brute force parallel searching method and the flow-based searching method, so as to promote the searching effect.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated in and form part of the specification in which like numerals designate like parts, illustrate preferred embodiments of the present invention and together with the description, serve to explain the principles of the invention. In the drawings:

Fig.1 is a perspective diagram of a prior art Security Policy Database;

Fig.2 is a perspective diagram of a prior art flow-based searching method;

Fig.3 is a perspective diagram of a prior art Patricia-based searching method;

Fig.4 is a flowchart for processing a prior art outbound IPSec;

Fig.5 is a flowchart for processing a prior art inbound IPSec;

Fig.6A is a flowchart for establishing peer-based Security Policy Databases according to the present invention;

Fig.6B is a flowchart to be performed when searching the security policy;

Fig.7 is a perspective diagram of a peer table according to the present invention;

Fig.8 is a perspective diagram of peer-based Security Policy Databases according to the present invention;

Fig.9 is a flowchart for processing an inbound IPSec packet in tunnel mode according to the present invention;

Fig.10 is a flowchart for processing an inbound IPSec packet in transport mode according to the present invention;

Fig.11 is a flowchart for processing an inbound IP packet according to the present invention; and

Fig.12 is a flowchart for processing an outbound IP packet according to the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

By means of the security gateway in tunnel mode, the embodiment of the present invention is described as follows.

An IPSec tunneling can be considered as a tunnel composed of an originating gateway and a terminating gateway. After the originating gateway performs the IPSec processing on the outbound packet transmitted out from the

internal network/local area network (LAN), an outer header is added. The source address of the outer header is the address of the originating gateway, and the destination address is the address of the terminating gateway. At this time, the terminating gateway is the peer gateway of the originating gateway.

On the other hand, the terminating gateway will take the packet as an inbound packet to enter into its internal network/local area network (LAN). After the terminating gateway removes the protection mechanism of the IPSec, the restored packet will be transmitted to the exact destination host. At this time, the terminating gateway will take the originating gateway as its peer gateway.

Therefore, it is reasoned that in the outer header of the inbound IPSec packet, the source address is the address of the external network/wide area network (WAN) of the peer gateway, and in the header of the inbound IP packet, the source address is within the internal network/local area network (LAN) of the peer gateway. In the header of the outbound IP packet, the destination address is within the internal network/local area network (LAN) of the peer gateway.

Therefore, by properly using the relation between the peer gateway and the packet, a peer table is established, and peer-based Security Policy Databases are built for each of the peer gateways so as to increase the searching speed of the Security Policy Database.

Fig.6A is a flowchart for establishing peer-based Security Policy Databases according to the present invention. In step S30, the method is initiated (S30). First, a peer table is established (S32), and then according to each of the peer gateways in the peer table, an exclusive peer-based Security Policy Database is built (S34). Fig.6B is a flowchart to be performed when searching the security policy. First, the peer table is searched (S36) so as to find out the corresponding

peer-based Security Policy Database. Then, the peer-based Security Policy Databases is searched (S38) so as to find out the security policy. Finally, the method is terminated (S40). Fig.7 is a perspective diagram of a peer table according to the present invention. The peer table comprises the fields of peer identification, address, prefix, and type.

The peer identification is directed to the pointer of the corresponding peer-based Security Policy Database. The address is the internal network/local area network (LAN) section or the external network/wide area network (WAN) address. The prefix represents the number of bits in the address to be compared for finding out the matching address. There are three kinds of types. One is I (the internal network/local area network (LAN) section type), another is E (external network/wide area network (WAN) address type), and another is B (both). Take the IP version 4 (IPv4) for example, the length of the prefix corresponding to the external network/wide area network (WAN) address is 32, and the length of the prefix corresponding to the internal network/local area network (LAN) address is within the rang of 1 to 32 depending on the size of the network section. The length of the prefix of the external network address is equal to the number of the address bits.

Each of the peer gateways in the peer table comprises two data, the external network/wide area network (WAN) address and the internal network/local area network (LAN) section of the peer gateway, which are separately expressed by the address, the prefix and the type. In Fig.7, as for the peer gateway of the peer identification 1, the external network/wide area network (WAN) address is 203.56.77.33, the internal network/local area network (LAN) section is 140.96.0.0, and the prefix is 16. Therefore, the range of internal network addresses of the peer gateway of the peer identification 1 is

from 140.96.0.0 to 140.96.255.255. Similarly, as for the peer gateway of the peer identification 2, the external network/wide area network (WAN) address is 207.52.79.40, the internal network/local area network (LAN) section is 140.112.0.0, and the prefix is 16. Therefore, the range of internal network addresses of the peer gateway of the peer identification 2 is from 140.112.0.0 to 140.112.255.255. Furthermore, the peer gateway of the peer identification 0 is a default peer gateway to be used by the remaining packets corresponding to no peer gateways, and both of its address and prefix are 0, and the type is B.

Fig.8 is a perspective diagram of peer-based Security Policy Databases according to the present invention. An exclusive Security Policy Database, called as peer-based Security Policy Database, is built for each of the peer gateways, and is used for storing the security policy relating to the peer gateway. The default peer gateway also has an exclusive peer-based Security Policy Database for storing the "by-pass" policy and the "discard" policy.

In Fig.1, the original Security Policy Database is linearly arranged. After the exclusive Security Policy Database is built for each of the peer gateways, as shown in Fig.8, the security policies relating to the peer gateway of the peer identification 1 are 1 and 5, and the security policies relating to the peer gateway of the peer identification 2 are 2, 3 and 4, and the security policy relating to the peer gateway of the peer identification 0 is 3. These security policies suitable to different peer gateways are separately arranged in a linear way so as to form independent peer-based Security Policy Databases.

When the security policy in Fig.1 is to be searched, it is searched from 1 to 5. If the security policy in Fig.8 is to be searched, it is required to search the peer identification from the peer table, and then to search the corresponding peer-based Security Policy Database. Therefore, the number of the security

policies to be searched will greatly decrease so as to save the searching time for the security policy.

When the user add a new policy in tunnel mode, the new policy will not only be added into the original Security Policy Database, but also added into the corresponding peer-based Security Policy Database if the new policy's peer gateway address is matching with the peer gateway address. The peer identification can be found out by searching the peer table's external network address. In order to maintain the policy order consistent with the original Security Policy Database, the source address or the destination address of the selectors of all of the newly-added policies have to be compared with the internal network/local area network (LAN) sections of other peer gateways so as to determine whether the overlapping occurs. If overlapped, the overlapped peer gateways have to add the new policy into its peer-based Security Policy Database. When the user wants to delete the policy, the user has to remove the data of the policy in the original Security Policy Database and in the peer-based Security Policy Database at the same time.

If the transport mode has to be supported at the same time, it is only required to take each of the peer hosts capable of directly communicating with the gateway as the peer gateway. First, at least one datum has to be built in the peer table for each of the peer hosts so as to store the network address of the peer host. The prefix is the same as the number of the address bits, and the type is B. Each of the peer host has an exclusive peer-based Security Policy Database established by using the above-mentioned way. Although in transport mode, the policy itself does not have the information for the peer gateway address, the policy will be within the peer-based Security Policy Database because of the overlapping between the destination address or the source

address of the selector and the peer host address.

In transport mode, the searching methods for the inbound IP packet and the outbound IP packet are the same as those in tunnel mode. However, the searching method for the inbound IPSec packet in transport mode is different from that in tunnel mode.

The procedure for processing the inbound IPSec packet in tunnel mode, the procedure for processing the inbound IPSec packet in transport mode, the procedure for processing the inbound IP packet, and the procedure for processing the outbound IP packet are separately described as the follows.

Fig.9 is a flowchart for processing an inbound IPSec packet in tunnel mode according to the present invention. As for the inbound IPSec packet, the first step is to remove the protection of the IPSec (S100). Then, the source address of the outer header of the inbound IPSec packet is compared with the external network/wide area network (WAN) address of the peer table (S102) so as to obtain the corresponding peer-based Security Policy Database. It not found, then no policy is found (S108). If found, the corresponding peer-based Security Policy Database is obtained. Therefore, the inner header of the inbound IPSec packet is compared with the policies in the peer-based Security Policy Database (S104) so as to obtain the policy matching with the condition or requirement. If the condition is matched, then the policy is found (S106). Otherwise, no policy is found (S108).

Fig.10 is a flowchart for processing an inbound IPSec packet in transport mode according to the present invention. As for the inbound IPSec packet, the first step is to remove the protection of the IPSec (S200). Then, the source address of the inbound IPSec packet is compared with the external network/wide area network (WAN) address of the peer table (S202) so as to

obtain the corresponding peer-based Security Policy Database. If not found, no policy is found (S208). Otherwise, the corresponding peer-based Security Policy Database is obtained. Therefore, the inbound IPSec packet is compared with the policies in the peer-based Security Policy Database (S204) so as to obtain the policy matching with the condition. If the condition is matched, the certain policy is found (S206). Otherwise, no policy is found (S208).

Fig.11 is a flowchart for processing an inbound IP packet according to the present invention. The source address of the inbound IP packet is compared with the internal network/local area network (LAN) section of the peer table (S300) so as to obtain the corresponding peer-based Security Policy Database. If not found, no policy is found (S306). Otherwise, the corresponding peer-based Security Policy Database is obtained, and then the inbound IP packet is compared with the policies in the peer-based Security Policy Database (S302) so as to obtain the policy matching with the condition. If the condition is matched, the certain policy is found (S304). Otherwise, no policy is found (S306).

Fig.12 is a flowchart for processing an outbound IP packet according to the present invention. First, the destination address of the outbound IP packet is compared with internal network/local area network (LAN) section of the peer table (S400) so as to obtain the corresponding peer-based Security Policy Database. If not found, then no policy is found (S406). If found, the corresponding peer-based Security Policy Database is obtained, and then the outbound IP packet is compared with the policies in the peer-based Security Policy Database (S402) so as to obtain the policy matching with the condition. If the condition is matched, the certain policy is found (S404). Otherwise, no policy is found (S406).

Furthermore, the present invention also can be combined with other improved SPD searching method, such as the brute force parallel searching method and the flow-based searching method. These two methods can be directly applied in all of the peer-based Security Policy Databases, or selectively applied in some of the peer-based Security Policy Databases, such the peer gateways with greater data flows.

When combined with the brute force parallel searching method, the inbound SPD and the outbound SPD are divided into multiple smaller inbound peer-based SPDs and multiple smaller outbound peer-based SPDs by using the provided method in the present invention. They are collectively managed by the policy manager, and the policy manager will transmit each of the searching requirement to the relating inbound peer-based SPDs or the relating outbound peer-based SPDs so as to performing the searching operation at the same time. Therefore, the searching requirements for the SPDs of the different peer gateways can be served at the same time so as to promote the system efficiency.

When combined with the flow-based searching method, the step of linearly searching the SPD for the first packet of each of the packet flows is replaced by the step of searching the peer-based Security Policy Database so as to decrease the delay caused by the searching.

Although the step of searching the peer gateway is further required in the present invention, the time complexity for searching the peer gateway is only O(1), no matter whether the hardware or software method is applied. Furthermore, by adding the step of searching the peer gateway, the average number of the policies in the peer-based Security Policy Database is 1/p of the original Security Policy Database, wherein p is the number of the peer gateways. Therefore, the time complexity for searching the Security Policy

Database is reduced to be O(n/p) in the average case.

Those skilled in the art will readily observe that numerous modifications and alterations of the device may be made while retaining the teachings of the invention. Accordingly, the above disclosure should be construed as limited only by the metes and bounds of the appended claims.